



07/13/04

AF/3621  
JFW  
\$

Patent No. 57760/03-642

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: George J. CANDELLA, et al.

Application No.: 09/710,776

Group No.: 3621

Filed: 11/09/2000

Examiner: Pierre E. Elisca

Confirmation No.: 5507

For: Method and System for Detecting Fraud in Non-Personal Transactions

Mail Stop Appeal Briefs – Patents

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF  
(PATENT APPLICATION--37 C.F.R. § 1.192)

1. Transmitted herewith, in triplicate, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on May 12, 2004.

2. STATUS OF APPLICANT

This application is on behalf of a small entity

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10\*

(When using Express Mail, the Express Mail label number is mandatory;  
Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

■ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)

□ with sufficient postage as first class mail.

37 C.F.R. § 1.10\*

■ as "Express Mail Post Office to Addressee"

Mailing Label No. EV399391135US (mandatory)

TRANSMISSION

□ facsimile transmitted to the Patent and Trademark Office, (703) \_\_\_\_\_

Nancy J. Moore  
Signature

Date: 7/12/04

Nancy J. Moore

(type or print name of person certifying)

\* Only the date of filing (§ 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under § 1.8 continues to be taken into account in determining timeliness. See § 1.703(f). Consider "Express Mail Post Office to Addressee" (§ 1.10) or facsimile transmission (§ 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 1.17(c), the fee for filing the Appeal Brief is:

small entity \$165.00

**Appeal Brief fee due \$165.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee \$165.00

Extension fee (if any) \$ 0.00

**TOTAL FEE DUE \$165.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of \$165.00 to Deposit Account No. 06-0540.

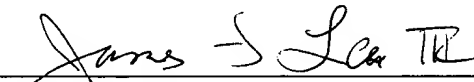
A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 06-0540.

Date: 7-12-09

Reg. No.: 41,143  
Tel. No.: 918-599-0621  
Customer No.: 22206

  
\_\_\_\_\_  
Signature of Practitioner

James F. Lea III  
FELLERS, SNIDER, BLANKENSHIP,  
BAILEY & TIPPENS, P.C.  
321 South Boston, Suite 800  
Tulsa, OK 74103-3318



Practitioner's Docket No. 57760/03-642

**PATENT**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of: George J. CANDELLA, et al.

Application No.: 09/710,776

Group No.: 3621

Filed: 11/09/2000

Examiner: Pierre E. Elisca

Confirmation No.: 5507

For: Method and System for Detecting Fraud in Non-Personal Transactions

**Mail Stop Appeal Briefs - Patents**

**Commissioner for Patents**

**P.O. Box 1450**

**Alexandria, VA 22313-1450**

**ATTENTION: Board of Patent Appeals and Interferences**

**APPELLANT'S BRIEF (37 C.F.R. § 1.192)**

This brief is in furtherance of the Notice of Appeal, filed in this case on May 12, 2004.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief is transmitted in triplicate. (37 C.F.R. § 1.192(a))

07/15/2004 HALI11 00000045 060540 09710776

01 FC:2402 165.00 DA

---

**CERTIFICATION UNDER 37 C.F.R. § 1.10**

I hereby certify that, on the date shown below, this correspondence is being deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 as "Express Mail Post Office to Addressee" Mailing Label No. EV399391135US.

Date: 7/12/04

Nancy J. Moore  
Nancy J. Moore

I. REAL PARTY IN INTEREST

The real party in interest is the party named in the caption of this brief.

II. RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal:

There are no such appeals or interferences.

III. STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims 1-32, which stand rejected.

B. STATUS OF ALL THE CLAIMS

1. Claims cancelled:	None
2. Claims withdrawn from consideration but not cancelled:	None
3. Claims pending:	1 – 32
4. Claims allowed:	None
5. Claims rejected:	1 – 32

C. CLAIMS ON APPEAL

The claims on appeal are claims 1 – 32.

IV. STATUS OF AMENDMENTS

No amendments were submitted subsequent to final rejection.

V. SUMMARY OF INVENTION

A method for detecting fraud in non-personal transactions comprising the steps of:

transmitting the purchaser's data to a fraud-detection system (100; Fig. 2)(page 6, line 9 – 12), the purchaser's data including a ship-to address for the transaction (118)(page 7, lines 10 – 13)(page 8, lines 1, 2).;

processing the purchaser's data to determine whether the transaction is potentially fraudulent (122, 124, 126, 128; Fig.3)(136, 140, 144, 146, 150; Fig. 4a)(156, 158, 159, 160, 161, 162, 163; Fig. 5A)(164, 165; Fig. 5B)(172, 174, 176, 178, 180, 182; Fig. 6)(128, 190, 192; Fig. 7)(130; Fig. 8)(page 6, lines 13 – 27); and

returning the relative risks of fraudulent activity associated with the transaction (240; Fig. 8)(page 6, lines 28 – page 7, line 9).

## VI. ISSUES

Whether claims 1 – 32 are unpatentable under 35 U.S.C. 102(e) over USPN 6,122,624 to Tetro et al.

## VII. GROUPING OF THE CLAIMS

Claims 1 – 32 stand or fall together.

## VIII. ARGUMENTS – REJECTIONS UNDER U.S.C. §102

The Examiner has rejected claims 1-32 as being anticipated by Tetro et al. (U.S. Pat. No. 6,122,624). Examiner states that,

“as per claims 1, 14-16, 24-27, and 31 Tetro discloses a method/system for enhanced fraud detection in electronic purchase transactions from a remote site (which is readable as Applicant's claimed invention wherein it is stated that a method for detecting fraud non-personal transactions), comprising the steps of:

transmitting the purchaser's data to a fraud-detection system, the purchaser's data including a ship-to-address for the transaction (see., abstract, specifically wherein it is stated that an electronic purchase is prompted to input the user's billing address and social security number, col 5, lines 47-59, the enhanced fraud detection system 10);

processing the purchaser's data to determine whether the transaction is potentially fraudulent (see., abstract, specifically wherein it is stated that a determination is made whether the account associated with the social security number has been authorized for use, col 2, lines 39-61, please note that the process for matching the user's billing address and social security number is equivalent to the step of determining for potential fraud);

returning the relative risk of fraudulent activity associated with the transaction (see., abstract, col 2, lines 49-67, specifically wherein it is stated that if the social security number falls into any of these categories, then authorization for the purchase is refused)."

Applicants respectfully disagree with the Examiner's assertion that Tetro et al. disclose a method/system comprising the steps of "transmitting the purchaser's data to a fraud-detection system, the purchaser's data including a ship-to-address for the transaction". The Examiner has noted correctly the teachings of Tetro et al. in the following sentence from the Office Action: "(see, abstract, specifically wherein it is stated that an electronic purchase is prompted to input the user's billing address and social security number, Col 5, lines 47-59, the enhanced fraud detection system 10)". As can be appreciated, even though the ultimate destination may be the same, the "ship-to-address" is stored as a first piece of data while the "user's billing address" is stored as a second piece of data. The importance of separately tracking the ship-to-address and the user's billing address is highlighted in the Applicants' "Background of the Invention" beginning on page 2, line 22 through page 3, line 4 which states,

The electronic merchant receives an order from the person who gives a name, credit card number, and expiration date to the retailer in connection with a purchase. The purchaser directs that the merchandise be delivered to an address which is different than the credit card billing address. Using traditional methods, the merchant receives a credit card approval number from its gateway and ships the merchandise to the shipping address.

If, in fact, the credit card number has been stolen and the transaction is fraudulent, the true cardholder will likely reject the invoice when he is billed for it, claiming fraud. Since the credit card company had confirmed the validity of the card (which remains in the owner's possession), and because the transaction is "card not present", i.e., was not involved with a signature verification, the credit card company has no liability. Assuming the cardholder refuses to pay the credit card company, the credit company will issue a charge back against the retailer, which has no recourse."

Transmitting the "ship-to address for the transaction", as is claimed in Applicants' novel method of claim 1, permits "checking the purchaser's ship-to address against a historical database to determine whether a pattern of fraudulent activity exists for the ship-to address; and checking the purchaser's ship-to address against a modeling engine to determine whether elements exist in the demographic data which correlate with fraudulent trends". (page 3, lines 21-26).

Checking the "ship-to address" provides benefits not available with other methods.

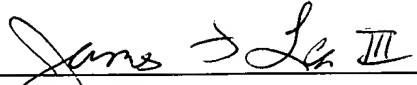
For example, if a merchant database reveals that there have been one or more deliveries to a specified ["ship-to"] address without objection by the cardholder, it is almost certain that further deliveries to that address (particularly if it matches the cardholder's address) are legitimate. If, however, a delivery is directed to an address inconsistent with the existing pattern associated with that critical purchase, it will trigger an alert that the transaction may be fraudulent. In such an event, the merchant will telephone or use the "safe-call" call verification program to communicate with the card owner to get confirmation of the bona fides of the transaction. (page 6, lines 13-27).

In conclusion, for at least the reasons set forth above, Applicants request allowance of claims 1-32 over the cited reference.

Date: 7-12-04

Reg. No.: 41,143  
Tel. No.: 918.599.0621  
Customer No.: 22206

W268269.1

  
James F. Lea III  
FELLERS, SNIDER, BLANKENSHIP,  
BAILEY & TIPPENS, P.C.  
321 South Boston, Suite 800  
Tulsa, OK 74103-3318





## IX. APPENDIX OF CLAIMS

1. Method for detecting fraud is non-personal transactions comprising the steps of:

transmitting the purchaser's data to a fraud-detection system, the purchaser's data including a ship-to address for the transaction;

processing the purchaser's data to determine whether the transaction is potentially fraudulent; and

returning the relative risks of fraudulent activity associated with the transaction.

2. The fraud detection method according to claim 1, wherein the processing step comprising parsing out the purchaser's ship-to address.

3. The fraud detection method according to claim 1, further comprising the step of checking to determine whether the purchaser's ship-to address exists.

4. The fraud detection according to claim 3, wherein the ship-to address checking step comprises comparing a zip code of the ship-to address against a post office database.

5. The fraud detection method according to claim 4, wherein the zip code is a ZIP + 4 zip code.

6. The fraud detection method according to claim 3, wherein the ship-to address checking step comprises comparing the city and state of the ship-to address against the city and state with the ZIP + 4 code.
7. The fraud detection method according to claim 3 wherein the ship-to address checking step comprises the area code of the purchaser's phone number to determine whether it fits the geographic area of the ship-to address.
8. The fraud detection method according to claim 3, wherein the ship-to address checking step comprises comparing the purchaser's ship-to address against the national change of address service database or the publisher's change of address database.
9. The fraud detection method according to claim 3, wherein the ship-to address checking step comprises rating the building site associated with the "ship-to" address to determine whether the building or lot type is inconsistent with the transaction data.
10. The fraud detection method according to claim 1, further comprising the step of checking the purchaser's ship-to address against an historical database to determine whether a prior history of fraud exists.

11. The fraud detection method according to claim 10, wherein the prior history of fraud determining step comprises checking whether a record associated with the purchaser's ship-to address exists in the historical fraud database.

12. The fraud detection method according to claim 11, wherein the associated record is checked to determine whether negative data is associated with the ship-to address.

13. The fraud detection method according to claim 1, further comprising the step of checking the purchaser's ship-to address against an historical database to determine whether a pattern of fraudulent activity exists for the ship-to address.

14. The fraud detection method according to claim 13, wherein the pattern of fraud detecting step comprises determining whether an overlapping use of payment means and ship-to address is present by consulting a database of prior transactions.

15. The fraud detection method according to claim 13, wherein the pattern of fraud detecting step comprises retroactively notifying the merchant of previous transactions associated with the ship-to address once a pattern of fraudulent activity has been detected.

16. The fraud detection method according to claim 1, further comprising the step of checking the purchaser's ship-to address against a modeling engine to determine whether elements exist in the demographic data which correlate with fraudulent trends.

17. The fraud detection method according to claim 1, further comprising the step of calculating a score based at least in part upon the likelihood that the transaction is fraudulent.

18. The fraud detection method according to claim 2, further comprising the step of checking to determine whether the purchaser's ship-to address exists.

19. The fraud detection method according to claim 18, wherein the ship-to address checking step comprises comparing a zip code of the ship-to address against a post office database.

20. The fraud detection method according to claim 19, wherein the zip code is a ZIP + 4 zip code.

21. The fraud detection method according to claim 18, wherein the ship-to address checking step comprises comparing the city and state of the ship-to address against the city and state with the ZIP + 4 code.

22. The fraud detection method according to claim 18, wherein the ship-to address checking step comprises checking the area code of the purchaser's phone number to determine whether it fits the geographic area of the ship-to address.

23. The fraud detection method according to claim 18, wherein the ship-to address checking step comprises comparing the purchaser's ship-to address against the national change of address service database or the publisher's change of address database.

24. The fraud detection method according to claim 18, wherein the ship-to address checking step comprises rating the building site associated with the "ship-to" address to determine whether the building or lot type is inconsistent with the transaction data.

25. The fraud detection method according to claim 18, further comprising the step of checking the purchaser's ship-to address against an historical database to determine whether a prior history of fraud exists.

26. The fraud detection method according to claim 25, wherein the prior history of fraud determining step comprises checking whether a record associated with the purchaser's ship-to address exists in the historical fraud database.

27. The fraud detection method according to claim 26, wherein the associated record is checked to determine whether negative data is associated with the ship-to address.

28. The fraud detection method according to claim 25, further comprising the step of checking the purchaser's ship-to address against an historical database to determine whether a pattern of fraudulent activity exists for the ship-to address.

29. The fraud detection method according to claim 28, wherein the pattern of fraud detecting step comprises determining whether an overlapping use of payment means and ship-to address is present by consulting a database of prior transactions.

30. The fraud detection method according to claim 28, wherein the pattern of fraud detecting step comprises retroactively notifying the merchant of previous transactions associated with the ship-to address once a pattern of fraudulent activity has been detected.

31. The fraud detection method according to claim 28, further comprising the step of checking the purchaser's ship-to address against a modeling engine to determine whether elements exist in the demographic data which correlate with fraudulent trends.

32. The fraud detection method according to claim 31, further comprising the step of calculating a score based at least in part upon the likelihood that the transaction is fraudulent.

W268892.1